(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 September 2005 (22.09.2005)

PCT

(10) International Publication Number
WO 2005/088440 A1

(51) International Patent Classification[7]: G06F 7/72

(21) International Application Number:
PCT/IB2005/050614

(22) International Filing Date: 18 February 2005 (18.02.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
04100873.1 4 March 2004 (04.03.2004) EP

(71) Applicant *(for DE only)*: **PHILIPS INTELLECTUAL PROPERTY & STANDARDS GMBH** [DE/DE]; Steindamm 94, 20099 Hamburg (DE).

(71) Applicant *(for all designated States except DE, US)*: **KONINKLIJKE PHILIPS ELECTRONICS N. V.** [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **AVANZI, Roberto** [IT/DE]; c/o Philips Intellectual Property & Standards GmbH, Weisshausstr. 2, 52066 Aachen (DE).

(74) Agent: **VOLMER, Georg**; Philips Intellectual Property & Standards GmbH, Weisshausstr. 2, 52066 Aachen (DE).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 2005/088440 A1

(54) Title: METHOD FOR THE EXPONENTIATION OR SCALAR MULTIPLICATION OF ELEMENTS

(57) Abstract: In orderr to further develop a method for the multi-exponentiation $(Ii_{i=1}{}^{d}\ g_i{}^{ei)}$ or the multi-scalar multiplication $(\Sigma_{i=1}{}^{d}$ *eigj)* of elements (g_j) by means of in each case at least one exponent or scalar (e_i), in particular an integer exponent or scalar, which has in each case a maximum bit rate *(n)* or bit length, in particular for the exponentiation (g^e) or scalar multiplication (e'g) of an element (g) by means of at least one exponent or scalar (*e*), in particular an integer exponent or scalar, which has in each case a maximum bit rate *(n)* or bit length, which elements (g_i; *g)* derive from at least one group (G), for example an Abelian group, which - in the case of (multi-)exponentiation is notated in particular multiplicatively and - in the case of (multi-)scalar multiplication is notated in particular additively, in such a way that the requirement in terms of storage space for recoded exponents or scalars (e_i) is reduced as much as possible even and especially in extremely restricted environments, such as in smart cards for example, the following method steps are proposed: [a.1] computing and storing or [a.2] retrieving from at least one memory all powers (g_i °) or all multiples (c'g_i), wherein c is a permissible positive coefficient; [b] dividing each exponent or scalar (e_i) into a number of chunks or into a number of parts (e_l,k) having a chunk or part width defined by a specific bit rate (*L*); and [c] individually recoding the chunks or parts ($e_{i,k}$).